UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/937,396	12/06/2001	Jean-Sebastien Coron	032326-169	9410

21839 7590 11/01/2005

BUCHANAN INGERSOLL PC
(INCLUDING BURNS, DOANE, SWECKER & MATHIS)
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
PATEL, NIRAV B	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 11/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/937,396	CORON, JEAN-SEBASTIEN	
	Examiner	Art Unit	
	Nirav Patel	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *9/29/2005 (Amendment)*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responding to the amendment dated 09/29/05.

2. Claims 1-13 are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 3, 5, 7, 9-11 and 12 are rejected under 35 U.S.C. 102(e) as being anticipated by Julio ("Improved Algorithms for Elliptic Curve Arithmetic in *GF (2^n), 1998*).

As per claim 1, Julio discloses:

an *elliptical curve type public key encryption algorithm* **[*page 1* "elliptic curve arithmetic"]**, wherein a point P on the elliptical curve is represented by *projective coordinates (X, Y, Z) such that x = X/Z and y = Z^3*, x and Y being the *coordinates of the point on the elliptical curve* in terms of affine coordinates **[*page 7* "projective point P = (X, Y, Z) has nonzero Z, then P can be represented by the projective point (x,**

y, 1), where x = X/Z and y = Y/Z^2"] said curve comprising n elements and being defined on a *finite field GF (p), where p is a prime number* and the curve has the *equation y^2 = x^3 + a*x + b*, or defined on a finite field GF (2^n) **[*page 2* "Elliptic curves over (GF (2^n)"]**, with the curve having the equation y^2 + x*y = x^3 + a*x^2 +b, where a and b are integer parameters **[page 7 "the projective equation of the affine equation $y^2 + xy = x^3 + ax^2 + b$"].**

drawing at random an integer λ such that 0 < λ < p **[page 7, 5.1, $\lambda \in$ GF (2^n), $\lambda \neq 0$]**;

a point P represented by projective coordinates (X1, Y1, Z1), *calculating* X'1 = λ^2*X1, Y'1 = λ^3*Y1 and Z'1 = λ*Z1, to define the *coordinates of the point P'* = (X'1, Y'1, Z'1) **[*page 7* "a projective plane P^2 is defined to be the set of equivalence classes of triple (X, Y, Z), not all zero, where (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) are said to be equivalent if there exists $\lambda \in$ GF (2^n), $\lambda \neq 0$ such that $X_1 = \lambda X_2$, $Y_1 = \lambda^2 Y_2$ and $Z_1 = \lambda Z_2$"];**

calculating an output point Q = 2P that is represented by projective coordinates (X2, Y2, Z2) **[*page 1* "the calculation of Q = mP, for P a point on the elliptic curve and m an integer, is the core operation of elliptic curve public-key cryptosystems" page 8 " the projective form of the doubling formula is 2 (X_1, Y_1, Z1) = (X_2, Y_2, Z_2)"].**

As per claim 3, the rejection of claim 1 is incorporated and further Julio disclose:

drawing at random a non-zero integer λ of GF (2^n) **[page 7, 5.1, $\lambda \in$ GF (2^n), $\lambda \neq 0$];**

replacing (i.e. set) X0 with λ^2*X0, Y0 with λ^3*Y0 and Z0 with λ*Z0 **[*page 6* "Set V ← x^2, D ← V, W ← Y, Set V ← V^2 +T"]**

calculating R = P + Q **[*page 12* "Output: projective coordinates (X_2, Y_2, Z_2) for the point $P_2 = P_0 + P_1$"].**

As per claim 5, the rejection of claim 1 is incorporated and is rejected for the same reason set forth in the rejection of claim 3 above.

As per claim 7, the rejection of claim 5 is incorporated and is rejected for the same reason set forth in the rejection of claim 3 above.

As per claim 9, the rejection of claim 1 is incorporated and further Julio disclose:

The algorithm returning as an output the $Q = d.P$ **[*page 1* "the calculation of Q = mP, for P a point on the elliptic curve and m an integer"]**, according to the following steps:

1) Initializing the point Q with the value P;

2) Replacing Q with 2.Q;

3) If d(t-1) = 1 replacing Q with Q+P;

4) For i ranging from t-2 to 0 executing the steps of:

4a) Replacing Q with 2Q;

4b) If d (i) = 1, replacing Q with Q+P; and

5) Returning Q **[*page 6* "Algorithm 1: Repeated doubling points"].**

As per claim 10, 11, 12, the rejection of claim 1 is incorporated. These claims are rejected for the same reason set forth in the rejection of claim 9 above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 2, 4, 6 and 8 are rejected under 35 USC 103 (a) for being unpatentable over Julio ("Improved Algorithms for Elliptic Curve Arithmetic in *GF (2^n), 1998*) and further in view of Jerome (" An Improved Algorithm for Arithmetic on a Family of Elliptic Curves" 1998).

As per claim 2, the rejection of claim 1 is incorporated and further Julio disclose:

the elliptical curve is defined on the finite field GF (p) (or GF (2^n), and the step of calculating Q **[*page 1* "in this paper we discuss efficient method for implementing elliptic curve arithmetic", The first method is new formula for doubling a point, i.e. for calculating the sum of equal point", "we also note that our formula can be applied to composite finite field as well", *Page 3* "Schroeppel [6] improved the doubling point formula saving the multiplication by the constant b" "3 A New Doubling Point Formula"].**

Julio doesn't explicitly disclose the singular algorithm to perform squaring, elliptic group operation, multiplication and addition-subtraction steps of the claim 2.

However, Jerome discloses the algorithm to perform squaring, elliptic group operation, multiplication and addition-subtraction **[*page 358* squaring, *page 359* group operation, *page 360* multiplication, *page 361* addition-subtraction method].**

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Jerome into the teaching of Julio to use the algorithm to perform different steps. The modification would be obvious because one of ordinary skill in the art would be motivated to do so because this improved version of the algorithm which runs 50% faster than any pervious version **[Jerome, *page 357*].**

As per claim 4, the rejection of claim 1 is incorporated and is rejected for the same reason set forth in the rejection of claim 2 and 3 above.

As per claim 6, the rejection of claim 1 is incorporated and is rejected for the same reason set forth in the rejection of claim 2.

As per claim 8, the rejection of claim 5 is incorporated and is rejected for the same reason set forth in the rejection of claim 2 and claim 3 above.

5. Claim 13 is rejected under 35 USC 103 (a) for being unpatentable over Julio ("Improved Algorithms for Elliptic Curve Arithmetic in *GF (2^n), 1998*) and further in view of Vanstone et al (US Patent No. 6,141,420).

As per claim 13, the rejection of claim 1 is incorporated and Julio doesn't disclose that electronics component is a smart cad.

However Vanstone discloses smart card (which utilize public key cryptography) **[*col. 1 lines 10-15* "the increasing use and sophistication of data transmission in such fields as telecommunications, networking, cellular communication, wireless communications, "smart card" applications, audio-visual and video communications has led to an increasing need for systems that permit data encryption, authentication and verification"].**

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Vanstone into the teaching of Julio to use public key cryptosystem in a smartcard. The modification would

be obvious because one of ordinary skill in the art would be motivated to use public key schemes, which reduce the size of the public key **[Vanstone, *col.1 lines 49-51*].**

Response to Argument

6. Applicant's arguments filed 9/29/05 have been fully considered but they are not persuasive.

Applicant argues that:

Lopez et al publication doesn't disclose random representative of a point on an elliptic curve, on which to perform a calculation [i.e. limitation of claim 1 (step 1) "drawing at random an integer λ such that $0 < \lambda < p$].

Examiner maintains that:

Lopes discloses that drawing at random an integer λ such that $0 < \lambda < p$ **[page 7 section 5.1 $\lambda \in$ GF (2^n), $\lambda \neq 0$ (i.e. $\lambda > 0$, it takes any primitive prime number in GF (2^n) which is consider to be random]** Furthermore, Lopez teaches that random integer mentioned above defines the coordinate of P' **[page 7, $X_1 = \lambda X_2$, $Y1 = \lambda^2 Y_2$ and $Z_1 = \lambda Z_2$ where P' represented by projective coordinates (X1, Y1, Z1) and P represented by projective coordinates (X2, Y2, Z2)].** Lopez teaches the "Improved Algorithm for Elliptical Curve Arithmetic in GF (2^n)" that provides the fastest known arithmetic on elliptical curves and also improves the running time for computing a scalar multiplication.

Applicant argues that:

Solinas publication doesn't disclose nor otherwise suggest this distinctive feature of the invention.

Examiner's response:

Solinas publication teaches that an Improved Algorithm for Arithmetic on a Family of Elliptic Curves **[see abstract]**. In response to applicant's argument, the fact that applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art cannot be the basis for patentability when the differences would otherwise be obvious. See *Ex parte Obiaya*, 227 USPQ 58, 60 (Bd. Pat. App. & Inter. 1985). Furthermore, the examiner recognizes that obviousness can only be established by combining or modifying the teaching of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to on of ordinary skill in the art. See *In re Fine*, 837 F. 2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and In re Jones, 958 F.2d 347, 21 USPQ 2nd 1941 (Fed. Cir 1992). In this case, the combination of **Lopez and Solinas teach the claimed subject matter and the combination is sufficient**. In fact, **Lopez and Solinas** do not need to disclose anything over and above the invention as claimed in order to render it unpatentable or anticipate. A recitation of the intended use of the claimed invention must result in structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention form the prior art. If the prior art structure is

capable of performing the intended use, then it meets the claimed limitations. For the above reasons, it is believed that the rejections should be sustained.

Examiner mentioned the Eric Von York ("Elliptic Curve over Finite Fields, 1992) publication in prior office action. Eric Von York teaches to determine the number of points on an elliptic curve E over a finite field. Furthermore, Eric Von York discusses the Hasse theorem (the Hasse theorem teaches picking points P uniformly and **randomly on an elliptic curve E (Fq)** in probabilistic polynomial time [See page 23 for further detail in Alfred J. Menezes ("Elliptic Curve Public key Cryptosystems" 1993) as mention in prior office action]).

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

NBP
10/21/05

Primary Examiner
Art Unit 2135